SWP-Aktuell
NR. 30 APRIL 2022

Die digitale Souveränität der EU ist umstritten

Warum die EU dennoch im EU-US-Handels- und -Technologierat auf den Brüssel-Effekt setzen sollte

Annegret Bendiek/Isabella Stürzer

Die starken wirtschaftlichen Verflechtungen zwischen der Europäischen Union (EU) und den USA erfordern eine enge Zusammenarbeit, wollen beide Partner auch im globalen digitalen Wettbewerb bestehen. Auf eine Initiative der EU hin wurde 2021 der Handels- und Technologierat (Trade and Technology Council, TTC) gegründet. Er soll dabei helfen, unterschiedliche Vorstellungen darüber zu überwinden, wie der digitale Markt und die Plattformökonomie am besten zu regulieren sind. Auch wenn der russische Angriff auf die Ukraine es notwendig macht, die strategische Souveränität der EU neu zu denken, sind europäische Entscheidungsträger und -trägerinnen gut beraten, weiterhin eine digitale Außenpolitik der EU voranzutreiben, die sich im Kern aus dem Ziel digitale Souveränität ableitet und die anstrebt, mithilfe des TTC europäische Regulierungen qua Marktmacht zu externalisieren. Dieser sogenannte »Brüssel-Effekt« vertieft nicht nur den transatlantischen digitalen Markt, sondern befördert gleichermaßen die Integration der EU-Digitalpolitik im Innern.

Seit 2015 betreibt die EU eine digitale Außenpolitik, die darauf abzielt, die Normen und Grundsätze ihrer Digitalpolitik zu externalisieren. Dieser Brüssel-Effekt basiert auf der Idee, dass Konflikte, die ihre Ursache in der divergierenden Auslegung grundlegender Normen und Prinzipien der internationalen Zusammenarbeit haben, durch Deliberation lösbar sind: Die Regulierung des digitalen Marktes erfolgt demnach nicht primär durch die Regierungen, sondern bezieht die großen Social-Media-Plattformen in die Politikformulierung mit ein. Dies führt dazu, dass Unternehmen ihre Geschäftsbedingungen an die EU-Binnenmarktstandards anpassen, und zwar unabhängig von der nationalen Gesetzgebung zur Digitalmarktregulierung. Sie lobbyieren sogar bei ausländischen Regierungen dafür, Rechtsvorschriften zu erlassen, die mit dem EU-Recht konvergieren, um die Rechtssicherheit zu erhöhen. Die Regulierungsmacht der EU in der digitalen Außenpolitik leitet sich aus ihrer Marktmacht ab, mit dem Ergebnis, dass außereuropäische Unternehmen aus dem Bereich digitale Technologien — vor allem solche mit Hauptsitz in den USA, aber auch in China — ihre Geschäftsbedingungen dahin-

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

gehend ändern, dass der Zugang zum europäischen Binnenmarkt gesichert bleibt.

Ein gutes Beispiel für den Brüssel-Effekt ist der EU-Verhaltenskodex für Cloud-Dienste (Cloud Code of Conduct, CCoC) aus dem Jahr 2021: Ihm entsprechend müssen nunmehr alle Cloud-Dienstleister zum Schutz personenbezogener Daten gemäß Artikel 28 der Datenschutz-Grundverordnung (DSGVO) hohe EU-Standards umsetzen. Dieser Kodex ist bisher weltweit einzigartig und hat sich als effizientes Regulierungsinstrument erwiesen, das die Einhaltung seiner Vorschriften gewährleistet, ohne rechtlich bindend zu sein. Allerdings wird nur solchen Unternehmen eine Genehmigung für den Betrieb von Cloud-Diensten im Binnenmarkt erteilt, die den Kodex erfüllen; bisher haben sich Unternehmen wie Alibaba, Alphabet, IBM und Microsoft an die Datenschutzbestimmungen gemäß dem CCoC gehalten. Dies zeugt von einer effizienten Multi-Stakeholder-Regulierung internationaler Serviceanbieter — denn die Europäische Kommission hat den Kodex in Zusammenarbeit mit privaten Unternehmen entwickelt.

Darüber hinaus sind die Bemühungen um die Formulierung und Umsetzung des CCoC bezeichnend für den Prozess einer europäischen Re-Souveränisierung unter den Bedingungen von Globalisierung und Digitalisierung (siehe Arbeitspapier FG EU / Europa, 2021/Nr. 01). Europas Regulierungsmacht setzt nicht nur die Standards einer digitalen Außenpolitik im transatlantischen Markt, sondern stärkt ebenso den Anspruch einer digitalen Souveränität der EU im Innern. Voraussetzung für eine erfolgreiche Externalisierung von EU-Regulierungen ist eine verbindliche Digitalpolitik, die im Innern von den Binnenmarktprinzipien getragen wird.

Die Souveränität der EU im digitalen Zeitalter

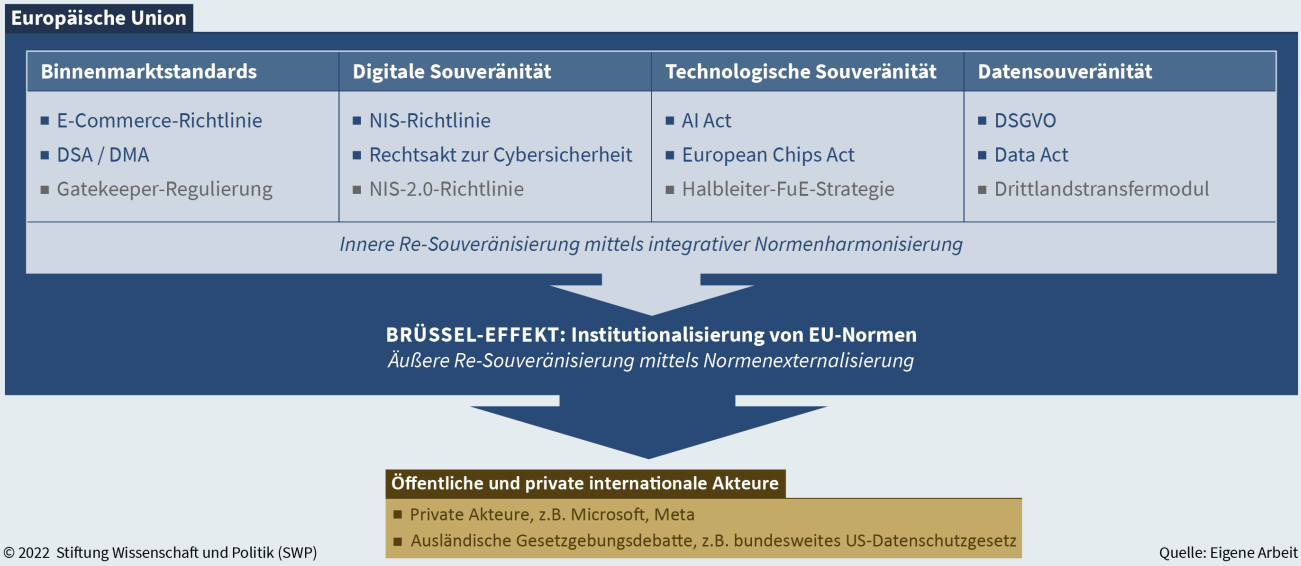
Erklärtes Ziel der gegenwärtigen EU-Kommission ist es, die »technologische Souveränität« und digitale Souveränität Europas zu sichern. Diese Begriffe hat erstmals die Industrie in die öffentliche Diskussion eingebracht, als Industrievertreter auf die technologische Verwundbarkeit der europäischen Gesellschaft und Wirtschaft hinwiesen: Europa mangele es an Produktionskapazitäten und Investitionen in Forschung und Entwicklung (FuE) von Schlüsseltechnologien. Die Verwundbarkeit kritischer technologischer Infrastrukturen wird hingegen als eine Frage der Cybersicherheit betrachtet und mit dem Begriff der »digitalen Souveränität« verknüpft. So ist es nicht verwunderlich, dass »digitale« und »technologische Souveränität« oftmals synonym verwendet werden.

Solche Diskussionen um verschiedene Aspekte von Souveränität zeigen, dass das Konzept von Souveränität im digitalen Zeitalter komplexer geworden ist und als politische Praxis europäischer Politikformulierung verstanden werden sollte. Souveränität bezieht sich nicht mehr nur auf einen rechtlich definierten Status, vielmehr muss sie im Kontext einer moderierenden Fähigkeit der EU gesehen werden, ihre Positionen durch transparente, interne Meinungsbildungsprozesse zu legitimieren. Der Anspruch der EU-Politikerinnen und -Politiker muss zudem das Ziel umfassen, diese Positionen in Multi-Stakeholder-Gremien und -Institutionen wie dem TTC effektiv zu externalisieren und somit auch die externe Souveränität der EU zu stärken.

Schlüsselinstrument der Re-Souveränisierung ist die auf europäischen Normen und Werten basierende Regulierungsmacht der EU: Intern kann die EU bei komplexen Fragen wie Haftungsverpflichtungen in der Plattformökonomie oder dem Datenschutz auf Social-Media-Plattformen Orientierung bieten; extern kann sie den Zugang zum Binnenmarkt an die Bedingung knüpfen, dass ihre Standards und Normen erfüllt werden. Dies erscheint recht voraussetzungsvoll, denn hierfür muss sie alle Marktakteure davon überzeugen, hohe ethische Standards einzuhalten und Verbraucherrechte zu schützen, sowie gleichzeitig einen fairen Marktwettbewerb, Unternehmenswachstum und Innovation ermöglichen. Im Idealfall schafft es die EU-Kommission, alle Markt-

Grafik

Digitale Souveränität der EU: Innere und äußere Dimension



Quelle: Eigene Arbeit

akteure an neue Marktregeln zu binden sowie zu gewährleisten, dass bestehende Marktregeln umgesetzt werden. Damit dies gelingen kann, müssen nicht nur die Kommission und der Ministerrat konstruktiv zusammenarbeiten, sondern auch Unternehmen, Interessengruppen und öffentliche Einrichtungen in Fragen von Interoperabilität und Haftungsverpflichtungen eng eingebunden werden.

Ein angemessenes Verständnis von europäischer Souveränität im digitalen Zeitalter umfasst dabei nicht nur die interne und die externe Dimension europäischen Handelns, sondern bezieht gleichermaßen die mitgliedstaatliche, die europäische und die internationale Ebene in die Formulierung der Digitalpolitik mit ein. Mit anderen Worten: Digitale Souveränität ist heute als politischer Mehrebenen-Prozess zu verstehen; ein enges territoriales und juristisches Verständnis von Souveränität greift eindeutig zu kurz.

Die Digitalpolitik der EU

Ein kurzer Überblick über die zentralen Säulen der digitalen Strategie der EU veranschaulicht, wie die EU ihre digitale Souveränität stärkt, indem sie ihre Grundwerte und Binnenmarktprinzipien (gegenseitige Anerkennung, unmittelbare Anwendbarkeit, Nichtdiskriminierung usw.) externalisiert (siehe Grafik). Hiermit gehen zwangsläufig Konflikte einher, da jede neue Regel und Vorschrift in erster Linie international operierende Unternehmen betrifft, von denen die meisten ihren Firmensitz in den USA oder in Asien (insbesondere Südkorea oder China) haben. Gleichzeitig hat die EU so auch die positive und negative europäische Integration vorangetrieben (vgl. SWP-Aktuell 71/2015).

Der Grundstein für eine digitale Außenpolitik der EU wurde 2016 mit der EU-Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) gelegt (siehe SWP-Aktuell 72/2017). Die NIS-Richtlinie verpflichtet Betreiber und Anbieter digitaler Dienste dazu, technische und organisatorische Mindeststandards zur Sicherung ihrer Netzwerke und Informationssysteme einzuhalten, um die Datensouveränität ihrer Nutzerinnen und Nutzer bestmöglich gewährleisten und im Falle von Sicherheitsvorfällen die zuständigen Behörden unverzüglich benachrichtigen zu können. Damit setzte diese Richtlinie internationale Standards in der Cybersicherheit. Seit 2021 wird eine Stärkung der NIS-Richtlinie (»NIS-2.0-Richt-

linie«) interinstitutionell verhandelt; ferner wird ausgelotet, ob diese Neufassung eine harmonisierte EU-weite Cyberregulierung ermöglichen und ein breiteres Verständnis von kritischen Infrastrukturen inkludieren könnte. An diesem Prozess sind neben EU-Institutionen verschiedenste Marktakteure beteiligt.

2019 hat das Europäische Parlament den EU-Rechtsakt zur Cybersicherheit verabschiedet, mit dem die EU-Cybersicherheitsagentur (ENISA) ein dauerhaftes Mandat zur Erhöhung der Cybersicherheitskapazitäten in der EU erhalten hat. Hiermit wurde erstmals ein einheitlicher Rahmen für die Zertifizierung von Informations- und Telekommunikationsprodukten und -diensten geschaffen, die Unternehmen auf dem europäischen Markt anbieten wollen (siehe SWP-Aktuell 60/2019).

Darüber hinaus veröffentlichte die Kommission im März 2019 eine Empfehlung zur 5G-Cybersicherheit, auf der die im Januar 2020 präsentierte Toolbox für sichere 5G-Netze im Wesentlichen basiert. Die Toolbox sieht vor, den Marktzugang für solche Telekommunikationsunternehmen zu kontrollieren, die sich um die Teilnahme an Aufbau und Betrieb nationaler 5G-Netze bewerben. Vor allem aus den USA, wo die Federal Communications Commission fünf Unternehmen (alle aus China) identifiziert hat, deren Produkte und Dienstleistungen als inakzeptables nationales Sicherheitsrisiko gelten, wurde Kritik laut, die Toolbox sei nicht strikt genug. Unterdessen haben einige europäische Regierungen und Firmen Bedenken im Hinblick auf das Prinzip der Anwenderneutralität geäußert; außerdem befürchten sie, die digitale Netzinfrastruktur im Binnenmarkt ohne Huawei nicht zügig weiterentwickeln zu können. Auch hier könnte sich eine vertiefte transatlantische Kooperation positiv auswirken, weil amerikanische Unternehmen durchaus Alternativen anbieten und zum europäischen Konnektivitätsausbau beitragen können.

Das Gesetz über künstliche Intelligenz (Artificial Intelligence [AI] Act) aus dem Jahr 2021 stellt den weltweit ersten Rechtsrahmen für die neue Schlüsseltechnologie künstliche Intelligenz (KI) dar. Es führt einen Risikobewertungsrahmen ein, der den Zugang zum europäischen Markt davon abhängig macht, wie die Risiken eingestuft werden, die mit dem Einsatz von KI(-Produkten) verbunden sein könnten. Europäische und internationale Unternehmen sehen zwar die Notwendigkeit eines einheitlichen rechtlichen Regelwerks, haben sich aber zugleich besorgt gezeigt, dass es auch innovationshemmend wirken könnte — denn wenn die vorgesehenen Bewertungskriterien streng ausgelegt würden, könnte die für die Rentabilität wichtige Vermarktung in der EU entfallen.

Durch die E-Commerce-Richtlinie von 2000 wurden bestimmte innerstaatliche Regelungen für die Dienste der Informationsgesellschaft EU-weit angeglichen. Auf diese Weise hat sie den freien Verkehr von Waren und Dienstleistungen im E-Commerce möglich gemacht, wobei sie Standards für Transparenzanforderungen für Dienstleister sowie für Haftungsregeln entlang der Lieferkette gesetzt hat. Noch in diesem Jahr soll die Richtlinie durch das Gesetz über digitale Dienste (Digital Services Act, DSA) und das Gesetz über digitale Märkte (Digital Markets Act, DMA) abgelöst werden.

Mit dem DSA werden zahlreiche neue Regeln eingeführt, die die Nutzung von digitalen Diensten transparenter machen sollen. Konkret geht es um Informationspflichten zur Speicherung und Kommerzialisierung von Nutzerdaten, um den Umgang mit Desinformation, das Aussprechen von Nutzungsverboten sowie die Möglichkeit, Personen zu melden, die illegale Inhalte teilen. Ergänzend zum DSA soll das DMA gleiche Wettbewerbsbedingungen für Unternehmen im digitalen Zeitalter schaffen, indem »große, systemische Online-Plattformen«, also sogenannte »Gatekeeper«, reguliert werden. Beispiele für Gatekeeper (obwohl bisher keine Unternehmen namentlich als solche benannt wurden) wären Amazon, Meta und Alphabet. Kleine und mittlere Unternehmen (KMU), die von diesen Gatekeepern abhängig sind, sollen durch das DMA geschützt werden, zum Beispiel indem den Plattformanbietern nicht mehr gestattet

sein soll, ihre eigenen Waren und Dienstleistungen prominenter zu bewerben als diejenigen anderer Anbieter. Überdies können kommerzielle Nutzer dann Zugang zu den Daten verlangen, die sie generieren, wenn sie die Dienste der Plattformen in Anspruch nehmen. Nicht zuletzt muss Dritten Interoperabilität ermöglicht werden.

In Ergänzung zu diesen Gesetzesinitiativen ist im Februar 2022 das Datengesetz (Data Act) vorgestellt worden, das festlegt, unter welchen Bedingungen personenbezogene Daten vermarktet werden dürfen.

Ein weiterer Baustein der europäischen digitalen und technologischen Re-Souveränisierung ist das Europäische Chip-Gesetz (European Chips Act) von 2022. Hiermit sollen nationale Investitionen in Forschung und Entwicklung von Chips eingebunden werden in eine kohärente europäische Halbleiterforschungsstrategie, ferner sollen kollektive Anstrengungen zum Aufbau von Halbleiterproduktionskapazitäten unternommen werden. Halbleiter sind entscheidende Komponenten zur Herstellung digitaler Technologien im zivilen ebenso wie im militärischen Bereich und derzeit so sehr nachgefragt, dass ein weltweiter Mangel herrscht. US-amerikanische Unternehmen wie der Marktführer Qualcomm entwerfen die Chips, hergestellt werden sie aber größtenteils im Ausland: So produziert ein einziges taiwanesisches Unternehmen vom derzeit fortschrittlichsten Chiptyp 92 Prozent des weltweiten Angebots. Auf Europa entfallen heute nur noch 10 Prozent der Marktanteile der weltweiten Chipindustrie; daher will die EU ihren Marktanteil bis 2030 auf 20 Prozent verdoppeln.

Durch die oben skizzierten Initiativen sollen die Wettbewerbsbedingungen im digitalen Binnenmarkt für alle Marktteilnehmer fairer gestaltet und der Schutz vor Cybersicherheitsbedrohungen erhöht werden. Damit schaffen sie notwendige, aber noch keine hinreichenden Bedingungen, um die digitale Souveränität Europas zu sichern. Diese lässt sich nur verbessern, wenn Produktionskapazitäten, große Unternehmen aus dem Bereich digitale Technologien sowie die erforderliche digitale Infrastruktur für eine enge transatlantische Kooperation vorhanden sind. Dafür braucht es sowohl eine den Aufbau europäischer Kapazitäten befördernde Industriestrategie als auch Kooperationsbereitschaft auf beiden Seiten des Atlantiks. Einen wichtigen Schritt, um die transatlantische Zusammenarbeit in der Chipproduktion zu vertiefen, markiert das kürzlich bekannt gegebene Vorhaben der US-Firma Intel, rund 80 Milliarden Euro in den Aufbau neuer Entwicklungs- und Produktionsstätten in Deutschland und Frankreich zu investieren. Allerdings ist es genauso bezeichnend, dass Europa selbst kein an Innovationskraft vergleichbares Unternehmen aufbieten kann.

Institutionalisierung des TTC

Trotz einzelner Konflikte in Zoll- und Handelsangelegenheiten bekennen sich die EU und die USA uneingeschränkt zu demokratischen Werten und fairem Marktwettbewerb. Beide Seiten müssen mit chinesischen Technologieunternehmen und -produkten konkurrieren und sind teils sogar von chinesischen Zulieferern abhängig. Angesichts dieser Herausforderungen schlug die EU-Kommission Mitte 2020 einen Handels- und Technologierat (TTC) vor. Während die Trump-Administration diesen Vorschlag nur wenig beachtete, nahm ihn die Biden-Administration unter der Maßgabe wieder auf, dass eine Allianz für demokratische Technologie geschaffen werde. Der TTC hat sich Ende September 2021 in Pittsburgh konstituiert und zehn Arbeitsgruppen eingerichtet; ein zweites Treffen ist für Mitte Mai 2022 noch während der französischen Ratspräsidentschaft in Frankreich geplant.

Der europäische Ansatz, mittels des TTC Standards zu institutionalisieren, trägt eindeutig die Handschrift der auf dem Brüssel-Effekt basierenden außenpolitischen Digitalstrategie der EU. Insofern ist nicht erstaunlich, dass das europäische Gesetz zur KI-Regulierung, das einen ethisch verantwortbaren Einsatz dieser Technologie garantieren soll, eine Debatte über seine aus US-Sicht gegebene innovationshemmende Wirkung

ausgelöst hat. Eine TTC-Arbeitsgruppe soll nun die recht weit gefasste Formulierung des Rechtsakts in detailliertere Anwendungsvorschriften übersetzen.

Ein Fall, in dem der Brüssel-Effekt sogar über die Regulierung privater Akteure hinausgeht und ausländische Gesetzgebungsdebatten prägt, ist die legislative Debatte über ein US-Bundesdatenschutzgesetz. Sie hat an Schwung gewonnen, nachdem einflussreiche Akteure wie Apple, Alphabet, Meta und Microsoft gemeinsam ein solches Gesetz ähnlich der DSGVO gefordert hatten. Die Tatsache, dass marktbeherrschende Technologieunternehmen an diesem Prozess beteiligt sind, ist ein Beleg für die Macht des Brüssel-Effekts:

Im Jahr 2020 drohten wichtige Führungskräfte von Meta damit, als Reaktion auf das Schrems-II-Urteil des Europäischen Gerichtshofs (EuGH) Plattformen wie Facebook und Instagram vom europäischen Markt zu nehmen. Als diese Taktik die europäische Position nicht wie gewünscht beeinflusste, nahmen sie die Androhung jedoch schnell wieder zurück. Meta erwirtschaftet 25 Prozent seines Umsatzes in Europa — ein zu großer Anteil, um ihn zu verlieren. Folglich musste der Konzern seine Geschäftsbedingungen und sein Geschäftsmodell für die Datenvermarktung an die europäischen Standards anpassen und plädiert nun für ein US-Bundesdatenschutzgesetz, das mit der DSGVO harmoniert. Eine derartige Lobbyarbeit durch private US-Unternehmen unterstreicht deren Interesse, mit der EU im TTC zusammenzuarbeiten, um gemeinsam digitale und technologische Standards zu setzen. Ziel der US-Firmen ist, ihren Marktzugang zu sichern und die Marktbedingungen zu ihren Gunsten mitzugestalten. Auch kleinere europäische Unternehmen können sich über eine eigens eingerichtete Online-Konsultationsplattform der Kommission einbringen in die transatlantische Kooperation im TTC.

So wie die EU von US-Technologie abhängig ist, sind gleichermaßen US-Unternehmen auf den Zugang zum weltweit größten Binnenmarkt — dem der EU — angewiesen. Dennoch bleiben für den TTC einige strittige Fragen zu klären.

Gatekeeper des digitalen Marktes

Zunächst ist umstritten, wie »Gatekeeper« definiert sind. Nach der Definition der EU fallen darunter in erster Linie außereuropäische Unternehmen wie Betreiber von Social-Media-Plattformen sowie digitale Marktplätze wie das amerikanische Amazon oder eBay und das chinesische Alibaba. Damit sind sie vom DSA und DMA betroffen. Die Einhaltung der Bestimmungen des DMA würde für diese Unternehmen bedeuten, ihre etablierten Geschäftsmodelle grundlegend ändern zu müssen. Bisher beruhen diese darauf, dass die Firmen Privatpersonen und kommerziellen Drittanbietern gestatten, ihre Plattformen im Austausch gegen ihre Daten kostenlos zu nutzen — dieses Geschäftsmodell hat die marktdominierende Stellung dieser Plattformen erst ermöglicht.

Da der Zugang zu den Marktplätzen kostenfrei ist, können Verbraucherinnen und Verbraucher über sie leicht ein KMU finden, das dort seine Produkte anbietet, und dann direkt bei diesem KMU einkaufen, oft zu einem günstigeren Preis. Für die Gatekeeper wiederum heißt das, dass sie ihre eigenen Produkte prominenter bewerben müssen, wollen sie ebenfalls profitieren. Diese Ausgangslage stellt das DMA vor das Dilemma, einerseits diskriminierende Praktiken von Marktführern verhindern zu wollen, andererseits nichtdiskriminierende Vorschriften erlassen zu müssen, um Datensouveränität und fairen Wettbewerb auf dem digitalen Markt zu gewährleisten.

Darüber hinaus haben US-Politikerinnen und -Politiker Sicherheitsbedenken geäußert, wenn Programme wie Apps außerhalb »geschlossener Systeme« verbreitet werden dürfen, wie es das DMA vorsieht; denn die Cybersicherheit digitaler Geräte könnte gefährdet werden, wenn Schadsoftware aus einer dritten Quelle heruntergeladen wird, die nicht den etablierten Prüf- und Verifizierungsverfahren unterliegt.

Die EU hat mit dem Erlass kartellrechtlicher Vorschriften für den digitalen Markt, wie dem DSA und dem DMA, einen Präzedenzfall geschaffen und damit die Agenda für die transatlantische Debatte gesetzt. Bei

den anstehenden Verhandlungen im TTC sollte die EU an dem durch das DSA und das DMA formulierten Regelungsrahmen festhalten und sowohl private Akteure als auch transatlantische Partner in die Gestaltung detaillierter sowie zusätzlicher Bestimmungen einbeziehen. Dieser Ansatz kann sich durchaus als effizient erweisen, zumal in den USA derzeit eine Kartellgesetzgebung diskutiert wird, die insbesondere große Technologieunternehmen betrifft.

In Anbetracht der Tatsache, dass digitale Dienstleistungen »unteilbar« sind, wie Anu Bradford es ausdrückt, haben US-Unternehmen bereits ihre Geschäftsbedingungen im Einklang mit der DSGVO aktualisiert, weil diese die weltweit strengste und detaillierteste Verordnung zum Datenschutz darstellt und es einfach zu kostspielig wäre, für jedes Land ein eigenes Dienstleistungsmodell anzubieten.

Schrems II und Rechtssicherheit

Ein weiterer Streitpunkt sind die geltenden Datenschutzbestimmungen nach der DSGVO, insbesondere seit der EuGH im Juli 2020 in der Rechtssache »Data Protection Commissioner gegen Facebook Ireland Limited und Maximilian Schrems« den »Privacy Shield« für ungültig erklärt hat, das heißt *das* transatlantische Abkommen, das den Austausch personenbezogener Nutzerdaten zwischen europäischen Tochterunternehmen und ihren amerikanischen Holdinggesellschaften zu Vermarktungszwecken regelte.

Als Reaktion auf das Urteil begann die Generalversammlung des EU Cloud CoC, der auch internationale Unternehmen angehören, mit der Arbeit an der Drittlandstransfer-Initiative, die darauf abzielt, Bedenken hinsichtlich der Verarbeitung personenbezogener Daten europäischer Nutzer und Nutzerinnen in einem Drittland auszuräumen. Dies soll geschehen, indem ein spezifisches Modul entwickelt wird, das die DSGVO ergänzen soll (»Drittlandstransfermodul«). Bislang wurde noch kein solches Modul für Drittländer eingeführt, da weiterhin unklar ist, wie es gestaltet sein könnte, um den Erwartungen des EuGH gerecht zu werden. Für fast zwei Jahre hat es die EU nun versäumt, einen neuen Rahmen zu schaffen, die Rechtsunsicherheiten für die betroffenen Unternehmen bestehen fort — und auch die am 25. März 2022 angekündigte prinzipielle Verständigung mit den USA über einen Ersatz für den Privacy Shield bleibt vorerst wenig konkret.

Dabei ist eine praktikable Lösung zur Schaffung von Rechtssicherheit für den transatlantischen Datentransfer dringend erforderlich. Um die Ersatzregelung für den Privacy Shield auszuarbeiten, könnte ein Aufsichtsgremium ernannt werden, das die Institutionalisierung des Drittlandstransfermoduls begleiten würde. Solche Aufsichtsbehörden können bei Nichteinhaltung von Vorgaben Geldstrafen verhängen und haben in der Vergangenheit erfolgreich vermittelt, wenn Unternehmenspraktiken (etwa von TikTok und Facebook) gegen DSGVO-Vorschriften verstießen.

Agendasetting in der transatlantischen Zusammenarbeit

Transatlantische Zusammenarbeit und europäische technologische Souveränität bedingen einander: So fordert das EU-Chipgesetz höhere öffentliche Investitionen in Halbleiter-FuE in Europa, während der im Juni 2020 verabschiedete amerikanische CHIPS for America Act Investitionen in Chipdesign-FuE in den USA vorsieht. Selbst wenn auf beiden Seiten des Atlantiks Bedenken über einen sich abzeichnenden, kontraproduktiven »Subventionswettlauf« vorgebracht wurden, könnte der Brüssel-Effekt ebenfalls in dieser Frage Abhilfe schaffen: Hier wie dort müssen sich Politikerinnen und Politiker darüber im Klaren sein, dass sich technologische Souveränität nicht zurückerlangen lässt, indem man sich nur auf sich selbst konzentriert — zu komplex sind internationale Interdependenzen in den Bereichen technologisches Know-how, Unternehmenskultur, Produktionsstätten und Ressourcenbeschaffung. Demzufolge wäre es naheliegend, auch Kanada künftig

in den TTC miteinzubeziehen, denn eine transatlantische demokratische Technologiepolitik wird spätestens dann nicht an Kanada vorbeikommen, wenn es um Ressourcensicherheit geht.

Da beide Chipgesetze erst vor kurzem erlassen worden sind, wäre es förderlich, die transatlantische Forschungszusammenarbeit zu erleichtern und — ähnlich wie bei der KI-Regulierung — sowohl Vorschriften für den Wettbewerb festzulegen (hier: auf dem Halbleitermarkt) als auch Zertifizierungskriterien (für Chipprodukte). Die Vorteile liegen gerade in Sicherheitsfragen auf der Hand, denn gemeinsam zertifizierte Chips im transatlantischen Markt sorgen für Vertrauen und könnten Spionage oder Sabotage durch Dritte weitestgehend vorbeugen.

Obwohl derzeit nur die USA über ausreichende Kapazitäten und Fachkenntnisse verfügen, um mit Unternehmen zu konkurrieren, deren Produkte aktuellen Zertifizierungsstandards nicht entsprechen (wie Huawei), kann die EU hier doch die Agenda der künftigen Zusammenarbeit im Hinblick auf demokratische Technologie und deren Steuerung bestimmen. Dies hat sie bei der KI-Technologie bereits mit Erfolg getan. Das Beispiel der Huawei-Geräte zeigt überdies, dass Unternehmen, die nicht bereit sind, die EU-Standards einzuhalten, damit rechnen müssen, vom Markt ausgeschlossen zu werden. Die EU sollte das betonen, wenn sie die Daten ihrer Bürgerinnen und Bürger auch vor US-Geheimdiensten schützen will.

Schlussfolgerungen und Ausblick

Amerikanische Firmen sind auf den Zugang zum europäischen Markt angewiesen, gleichzeitig sind Marktteilnehmer und -teilnehmerinnen im EU-Binnenmarkt hochgradig abhängig von den Produkten amerikanischer Digitaltechnikunternehmen. Gemeinsam bilden USA und EU den größten Markt, dessen einzelne Länder auch liberale Demokratien sind, und teilen zentrale Werte wie Schutz der Menschenrechte, Rechtsstaatlichkeit und freien, fairen wirtschaftlichen Wettbewerb. All dies spricht für eine enge transatlantische Zusammenarbeit in Fragen der Digitalisierung, der Technologie-Governance und bei der Entwicklung von demokratischer Technologie.

Europäische Entscheidungsträgerinnen und -träger sind gut beraten, in Vorbereitung der Mai-Tagung des TTC das Ziel zu formulieren, die anspruchsvollen europäischen Standards für fairen Wettbewerb und hohen Datenschutz zu gewährleisten und sich dafür den Brüssel-Effekt zunutze zu machen. Gleichzeitig ist es wichtig, offen zu bleiben für Verhandlungen in Detailfragen, denn einzelne Bestimmungen wie die namentliche Nennung von Gatekeepern mittels des DMA können und müssen noch weiter diskutiert und konkretisiert werden. Die EU hat hier einen Rahmen für den digitalen Markt vorgegeben und sollte diesen ihren Ansatz unter Einbeziehung von Interessengruppen weiterverfolgen. Es gilt, die neuen Vorschriften so anzupassen, dass sie in der Unternehmenspraxis umsetzbar sind.

Um mit einer kohärenten Strategie und einem glaubwürdigen Mandat in die Verhandlungen gehen zu können — und damit in der Lage zu sein, Europas digitale Souveränität auch gegenüber den USA zu behaupten —, ist es von entscheidender Bedeutung, den Prozess der internen europäischen Re-Souveränisierung weiter voranzutreiben, indem man sich in der EU schnellstmöglich auf ein Rechtssubstitut für den Privacy Shield einigt. EU-Verordnungen, die im Rahmen der europäischen Komitologieverfahren entwickelt wurden, sind in der Vergangenheit trotz anfänglich heftiger Widerstände erfolgreich über den Brüssel-Effekt externalisiert worden. An diesem Vorgehen sollte sich die EU orientieren und auf diesem Wege ebenso die eigene Integration vertiefen.

Dr. Annegret Bendiek ist Stellvertretende Leiterin der Forschungsgruppe EU/Europa.
Isabella Stürzer ist studentische Mitarbeiterin in der Forschungsgruppe EU/Europa.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3—4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1611-6364
ISSN (Online) 2747-5018
doi: 10.18449/2022A30

(Leicht gekürzte deutsche Version von SWP Comment 20/2022)